RYSZARD RADZIEJEWSKI
Wojskowa Akademia Techniczna
Warszawa

Infrastruktura krytyczna – kolejne resortowe królestwo?

Tematyka bezpieczeństwa narodowego, chociaż rzadko nazywana po imieniu, ostatnimi czasy cieszy się olbrzymim i nieustającym zainteresowaniem polityków i mediów. Byłby to powód do zadowolenia, gdyby nie kontekst tego zainteresowania: najpierw katastrofa prezydenckiego samolotu na lotnisku w Smoleńsku – śmierć Głowy Państwa, wielu szefów najważniejszych instytucji oraz dowództwa sił zbrojnych, później powodzie, które obnażyły nie tylko wieloletnie zaniedbania w ochronie przeciwpowodziowej, ale przede wszystkim brak systemowego podejścia do ochrony infrastruktury krytycznej.

Infrastruktura krytyczna (IK) to wszelkie urządzenia hydrotechniczne, w tym wały przeciwpowodziowe, o których obronę toczyły się heroiczne batalie, ponieważ w ustawie „O zarządzaniu kryzysowym" jest ona określona jako „systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców"[1]. Bez wątpienia zniszczenia wałów zagroziły bezpieczeństwu obywateli i zakłóciły sprawne funkcjonowanie administracji publicznej, instytucji oraz przedsiębiorstw na zalanych terenach.

Zapowiedzi polityków podjęcia zdecydowanych działań mających na celu uzdrowienie sytuacji należy jednak traktować z wielką dozą nieufności, wszakże już wcześniej stan naszej infrastruktury krytycznej był testowany przez siły natury, np. nocne opady mokrego śniegu, które spowodowały uszkodzenia m.in. dwóch linii energetycznych zasilających Szczecin: „Zimne kaloryfery, kran, z którego pociekło tylko kilka kropli, głuchy telefon, milczące telewizor i radio – tak dla ponad 300 tysięcy ludzi rozpoczął się wtorkowy poranek […] Wygasły ekrany bankomatów. Większość sklepów zamknięto, choć wyjątkowo fiskus zezwolił na sprzedaż bez działających kas fiskalnych"[2]. „Przez cały dzień miasto wyglądało jak opuszczone. Mały ruch, martwe światła sygnalizacyjne. Sporo policji i żandarmerii"[3]. Te lekcje pokory udzielone przez siły natury dobitnie wskazują, że niewiele czynimy, aby zapobiegać skutkom klęsk żywiołowych. Powstaje pytanie: co by było, gdyby nie tylko stan, ale i poziom ochrony infrastruktury krytycznej zechcieli przetestować np. terroryści?

Skutki zapewne byłby opłakane, więc cieszy, że w cieniu szumnych zapowiedzi polityków problematyka ochrony infrastruktury krytycznej jest kontynuowana: w końcu kwietnia 2010 roku weszły w życie trzy – jakże ważne – rozporządzenia Rady Ministrów:

[1] *Ustawa o zarządzaniu kryzysowym z 26 kwietnia 2007 r.*, „Dziennik Ustaw RP" (dalej – Dz.U.) 2007, nr 89, poz. 590, art. 3, pkt 2.
[2] M. Stankiewicz, *Gwałtowny atak zimy sparaliżował Szczecin*, „Rzeczpospolita" 2009, nr 84.
[3] A. Kraśnicki, *Szczecin przeżył ciemność*, „Gazeta Wyborcza" 2009, nr 84.

w sprawie raportu o zagrożeniach bezpieczeństwa narodowego[4], w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej[5] i w sprawie planów ochrony infrastruktury krytycznej[6].

Rozporządzenie w sprawie raportu o zagrożeniach bezpieczeństwa narodowego określa sposób, tryb i terminy jego opracowania przez ministrów kierujących działami administracji rządowej, kierowników urzędów centralnych oraz wojewodów na podstawie raportów cząstkowych, które będą obejmowały m.in.: najważniejsze zagrożenia i skutki ich wystąpienia; cele strategiczne, jakie należy osiągnąć, aby zminimalizować możliwość wystąpienia zagrożeń lub ich skutków; wskazanie sił i środków niezbędnych do osiągnięcia celów strategicznych; programowanie zadań w zakresie poprawy bezpieczeństwa państwa; określenie priorytetów w reagowaniu na określone zagrożenia.

Rozporządzenie w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej określa sposób realizacji obowiązków i współpracy przez organy administracji publicznej i służby odpowiedzialne za bezpieczeństwo narodowe z właścicielami oraz posiadaczami samoistnymi i zależnymi obiektów, instalacji, urządzeń i usług infrastruktury krytycznej.

Rozporządzenie w sprawie planów ochrony infrastruktury krytycznej określa sposób ich tworzenia, aktualizacji i strukturę, opracowywanych przez właścicieli oraz posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej, a także warunki i tryb uznania spełnienia obowiązku posiadania planu odpowiadającego wymogom planu ochrony infrastruktury krytycznej.

Rozporządzenia są dopełnieniem stosownych zapisów w ustawie „O zarządzaniu kryzysowym" i można by sądzić, że problematyka ochrony infrastruktury krytycznej pojawia się w naszym ustawodawstwie dopiero za sprawą tej ustawy. Nic bardziej błędnego – infrastruktura krytyczna była i jest chroniona na mocy innych ustaw. Wydaje się, że nie dostrzegają tego pracownicy Rządowego Centrum Bezpieczeństwa (RCB), które kontynuuje prace zainicjowane przed kilku laty w Departamencie Zarządzania Kryzysowego MSWiA, zmierzające do opracowania „Krajowego planu ochrony infrastruktury krytycznej".

Patrzenie na ochronę IK tylko przez pryzmat ustawy „O zarządzaniu kryzysowym" musi budzić niepokój – obyśmy nie mieli kolejnego „resortowego królestwa" w dziedzinie bezpieczeństwa (tego określenia użył szef Biura Bezpieczeństwa Narodowego, Władysław Stasiak, w odniesieniu do sfery bezpieczeństwa narodowego[7]). Ochrona IK wymaga zaangażowania wszystkich resortów odpowiedzialnych za bezpieczeństwo narodowe, a przede wszystkim ujednolicenia aktów prawnych.

Ochrona infrastruktury krytycznej w polskim ustawodawstwie

W Polsce termin „infrastruktura krytyczna" pojawił w 2002 roku w związku z pracami realizowanymi w ramach NATO. Początkowo określono ją jako „zespół podstawowych urządzeń i instytucji usługowych niezbędnych do należytego funkcjonowania produkcyjnych działów gospodarki"[8]. Termin ten jest stosunkowo nowy, powstał na początku lat dziewięćdziesiątych po wielkich awariach sieci energetycznych w Stanach Zjednoczonych i Kanadzie i odnosił się do systemów oraz instalacji niezbędnych do funkcjonowania nowoczesnego społeczeństwa i administracji. W miarę zmiany istoty za-

[4] *Rozporządzenie Rady Ministrów z 30 kwietnia 2010 r. w sprawie raportu o zagrożeniach bezpieczeństwa narodowego*, Dz.U. 2010, nr 83, poz. 540.
[5] *Rozporządzenie Rady Ministrów z 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej*, *ibidem*, poz. 541.
[6] *Rozporządzenie Rady Ministrów z 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej*, *ibidem*, poz. 542.
[7] A. Walentek, *Zbierać i analizować informacje*, „Życie Warszawy" z 26 sierpnia 2006 r.
[8] W. Wojciechowicz, *Ochrona infrastruktury krytycznej państwa*, „Myśl Wojskowa" nr 1 z 2004 r.

grożeń, zwłaszcza po atakach terrorystycznych 11 września 2001 roku, obejmował coraz szersze sfery infrastruktury państw, w tym i tych stowarzyszonych w Unii Europejskiej.

W czerwcu 2004 roku Rada Europejska wezwała do przygotowania ogólnej strategii ochrony infrastruktury krytycznej. W odpowiedzi 20 października 2004 roku Komisja wydała komunikat zawierający propozycje usprawnienia europejskich systemów zapobiegania atakom terrorystycznym wymierzonym przeciwko infrastrukturze krytycznej, a także zwiększenia gotowości i zdolności do reagowania na takie ataki[9]. 17 listopada 2005 roku Komisja przyjęła tzw. Zieloną Księgę (Green Paper on European Programme for Critical Infrastructure Protection), w której przedstawiono opcje polityczne dotyczące opracowywania tego programu oraz sieci ostrzegania o zagrożeniach dla infrastruktury krytycznej[10].

W grudniu 2005 roku Rada ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych wezwała Komisję do przygotowania wniosku dotyczącego utworzenia europejskiego programu ochrony infrastruktury krytycznej (EPOIK), uwzględniającego wszystkie rodzaje zagrożeń: wywołane działalnością człowieka, technologiczne i katastrofy naturalne, najwięcej jednak uwagi poświęcając zagrożeniom terrorystycznym.

W 2007 roku Rada przyjęła wnioski w sprawie EPOIK, w których podkreśliła: „Główna odpowiedzialność za ochronę infrastruktury krytycznej spoczywa na państwach członkowskich, właścicielach, operatorach i użytkownikach (użytkowników definiuje się jako organizacje eksploatujące i wykorzystujące infrastrukturę do celów gospodarczych i do celów świadczenia usług)"[11]. Konsekwencją dalszych prac była dyrektywa określana jako pierwszy krok w etapowym podejściu do rozpoznania i wyznaczenia europejskiej infrastruktury krytycznej (EIK) oraz do oceny potrzeb w zakresie poprawy jej ochrony. Za sektory priorytetowe uznano energetyczny i transportu, które w pierwszej kolejności powinny zostać poddane przeglądowi, aby ocenić skutki zakłócenia ich pracy, a także określić kolejne sektory, m.in. technologii informacyjno-komunikacyjnych (TIK)[12]. Został on opisany w 2009 roku w komunikacie Komisji do: Parlamentu Europejskiego, Rady Europy, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, w sprawie ochrony krytycznej infrastruktury informatycznej[13].

Konsekwencją ustaleń Rady, a także art. 113 „Strategii bezpieczeństwa narodowego Rzeczypospolitej Polskiej"[14] („Odpowiedzią na wzrastający poziom zagrożeń wobec obiektów i systemów infrastruktury, która ma kluczowe znaczenie dla bezpieczeństwa państwa i jego mieszkańców, powinny być działania ukierunkowane na stworzenie mechanizmu ochrony narodowej infrastruktury krytycznej. Należy dążyć do opracowania narodowego planu ochrony infrastruktury krytycznej oraz zaangażowania w proces budowy mechanizmu – poza administracją i służbą publiczną – także operatorów i właścicieli infrastruktury, w tym prywatnych. Mając świadomość ponadnarodowego wymiaru funkcjonowania infrastruktury krytycznej, należy zapewnić aktywny udział Polski w pracach nad jej ochroną, toczących się na forum NATO i UE") było podjęcie w Polsce w 2007 roku prac związanych z utworzeniem „Krajowego planu ochrony infrastruktury krytycznej", któ-

[9] Komisja Wspólnot Europejskich, Bruksela, 20.10.2004, COM (2004) 702, końcowy.
[10] Komisja Wspólnot Europejskich, Bruksela, 17.11.2005, COM (2005) 576, końcowy.
[11] *Decyzja Rady z 12 lutego 2007 r. ustanawiająca na lata 2007–2013, jako część ogólnego programu w sprawie bezpieczeństwa i ochrony wolności szczegółowy program „Zapobieganie, gotowość i zarządzanie skutkami terroryzmu i innymi rodzajami ryzyka dla bezpieczeństwa"*, „Dziennik Urzędowy Unii Europejskiej" (dalej – Dz.Urz. UE) L.07.58.1, pkt 10.
[12] *Dyrektywa Rady 2008/114/WE z 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony*, *ibidem* L.08.345.75.
[13] *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-społecznego i Komitetu Regionów w sprawie ochrony krytycznej infrastruktury informatycznej „Ochrona Europy przed zakrojonymi na szeroką skalę atakami i zakłóceniami cybernetycznymi: zwiększenie gotowości, bezpieczeństwa i odporności"*, Bruksela, 30.3.2009, COM (2009) 149, wersja ostateczna.
[14] *Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej*, Warszawa 2007.

ry miał stworzyć spójny system zarządzania bezpieczeństwem infrastruktury krytycznej w kraju, obejmując wszystkie istotne dla funkcjonowania państwa, gospodarki i społeczeństwa sektory, a także dostarczyć narzędzia zwiększające poziom bezpieczeństwa i minimalizujące straty będące konsekwencją szerokiego spektrum zagrożeń[15].

Wprawdzie plan taki nie powstał, ale problematyka ochrony infrastruktury krytycznej została ujęta w ustawie „O zarządzaniu kryzysowym". Określono w niej, że infrastruktura krytyczna to „systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców"[16].

Obejmuje ona systemy:

- zaopatrzenia w energię i paliwa;
- łączności i sieci teleinformatycznych;
- finansowe;
- zaopatrzenia w żywność i wodę;
- ochrony zdrowia,;
- transportowe i komunikacyjne;
- ratownicze;
- zapewniające ciągłość działania administracji publicznej;
- produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

Analizując składniki infrastruktury krytycznej wymienione w ustawie „O zarządzaniu kryzysowym", w krajowym ustawodawstwie można znaleźć jej odpowiedniki, określone jako: „obiekty podlegające obowiązkowej ochronie" oraz „obiekty szczególnie ważne dla bezpieczeństwa i obronności państwa". Wielka szkoda, że tego nie dostrzeżono podczas prac nad ustawą „O zarządzaniu kryzysowym", że nie zadano sobie pytania: jak dotychczas (do momentu wejścia w życie ustawy „O zarządzaniu kryzysowym") były chronione obiekty infrastruktury krytycznej, bo nie ulega wątpliwości, że były i nadal są chronione – jako „obiekty podlegające obowiązkowej ochronie".

Co kryje się pod określeniami „obiekty podlegające obowiązkowej ochronie" oraz „obiekty szczególnie ważne dla bezpieczeństwa i obronności państwa", na ile są one tożsame z definicją infrastruktury krytycznej?

O obiektach podlegających obowiązkowej ochronie traktuje ustawa „O ochronie osób i mienia"[17], gdzie w art. 5 określono obszary, obiekty i urządzenia ważne dla obronności, interesu gospodarczego państwa, bezpieczeństwa publicznego i innych ważnych interesów państwa, podlegające obowiązkowej ochronie przez specjalistyczne uzbrojone formacje ochronne lub odpowiednie zabezpieczenie techniczne.

Do tych obszarów, obiektów i urządzeń należą:

1. w zakresie obronności państwa:
   - zakłady produkcji specjalnej oraz zakłady, w których prowadzone są prace naukowo-badawcze lub konstruktorskie w zakresie takiej produkcji;
   - zakłady produkujące, remontujące i magazynujące uzbrojenie, urządzenia i sprzęt wojskowy;
   - magazyny rezerw państwowych;
2. w zakresie ochrony interesu gospodarczego państwa:
   - zakłady mające bezpośredni związek z wydobyciem surowców mineralnych o znaczeniu strategicznym;
   - porty morskie i lotnicze;

[15] R. Radziejewski, *Infrastruktura krytyczna*, „Przegląd Obrony Cywilnej" 2007, nr 7.
[16] *Ustawa o zarządzaniu kryzysowym*..., art. 3, pkt 2.
[17] *Ustawa o ochronie osób i mienia z 22 sierpnia 1997 r.*, Dz.U. 1997, nr 114, poz. 740.

- banki i przedsiębiorstwa wytwarzające, przechowujące bądź transportujące wartości pieniężne w znacznych ilościach;

3. w zakresie bezpieczeństwa publicznego:
   - zakłady, obiekty i urządzenia mające istotne znaczenie dla funkcjonowania aglomeracji miejskich, których zniszczenie lub uszkodzenie może stanowić zagrożenie dla życia i zdrowia ludzi oraz środowiska, w szczególności elektrownie i ciepłownie, ujęcia wody, wodociągi i oczyszczalnie ścieków;
   - zakłady stosujące, produkujące lub magazynujące w znacznych ilościach materiały jądrowe, źródła i odpady promieniotwórcze, materiały toksyczne, odurzające, wybuchowe bądź chemiczne o dużej podatności pożarowej lub wybuchowej;
   - rurociągi paliwowe, linie energetyczne i telekomunikacyjne, zapory wodne i śluzy oraz inne urządzenia znajdujące się w otwartym terenie, których zniszczenie lub uszkodzenie może stanowić zagrożenie dla życia lub zdrowia ludzi, środowiska albo spowodować poważne straty materialne;
4. w zakresie ochrony innych ważnych interesów państwa:
   - zakłady o unikalnej produkcji gospodarczej;
   - obiekty i urządzenia telekomunikacyjne, pocztowe oraz telewizyjne i radiowe;
   - muzea i inne obiekty, w których zgromadzone są dobra kultury narodowej;
   - archiwa państwowe.

O obiektach szczególnie ważnych dla bezpieczeństwa i obronności państwa traktuje rozporządzenie Rady Ministrów z 24 czerwca 2003 roku[18], które określa ich kategorie, a także zadania w zakresie ich szczególnej ochrony oraz właściwość organów w tych sprawach.

W rozumieniu tego rozporządzenia są to:

- zakłady produkujące, remontujące i magazynujące uzbrojenie i sprzęt wojskowy oraz środki bojowe, a także te, w których są prowadzone prace badawczo-rozwojowe lub konstruktorskie w zakresie produkcji na potrzeby bezpieczeństwa i obronności państwa;
- magazyny rezerw państwowych, w tym bazy i składy paliw płynnych, żywności, leków i artykułów sanitarnych;
- obiekty jednostek organizacyjnych podległych ministrowi obrony narodowej lub przez niego nadzorowanych;
- obiekty infrastruktury transportu samochodowego, kolejowego, lotniczego, morskiego i wodnego śródlądowego, drogownictwa, kolejnictwa i łączności oraz ośrodki dokumentacji geodezyjnej i kartograficznej;
- zapory wodne i inne urządzenia hydrotechniczne;
- obiekty jednostek organizacyjnych Agencji Wywiadu;
- obiekty: Narodowego Banku Polskiego oraz Banku Gospodarstwa Krajowego i Polskiej Wytwórni Papierów Wartościowych S.A. oraz Mennicy Państwowej S.A.;
- obiekty, w których produkuje się, stosuje lub magazynuje materiały jądrowe oraz źródła i odpady promieniotwórcze;
- obiekty telekomunikacyjne przeznaczone do nadawania programów radia publicznego i telewizji publicznej;
- obiekty organów i jednostek organizacyjnych podległych ministrowi właściwemu do spraw administracji publicznej lub przez niego nadzorowanych;
- obiekty organów i jednostek organizacyjnych podległych ministrowi właściwemu do spraw wewnętrznych lub przez niego nadzorowanych;

[18] *Rozporządzenie Rady Ministrów z 24 czerwca 2003 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony*, *ibidem* 2003, nr 116, poz. 1090.

- obiekty jednostek organizacyjnych Agencji Bezpieczeństwa Wewnętrznego;
- obiekty Policji, Straży Granicznej i Państwowej Straży Pożarnej;
- obiekty znajdujące się we właściwości ministra sprawiedliwości, Służby Więziennej oraz jednostek organizacyjnych podległych lub nadzorowanych przez ministra sprawiedliwości;
- zakłady mające bezpośredni związek z wydobywaniem kopalin podstawowych;
- obiekty, w których produkuje się, stosuje lub magazynuje materiały stwarzające szczególne zagrożenie wybuchowe lub pożarowe;
- obiekty, w których prowadzi się działalność z wykorzystaniem toksycznych związków chemicznych i ich prekursorów, a także środków biologicznych, mikrobiologicznych, mikroorganizmów, toksyn i innych substancji wywołujących choroby u ludzi lub zwierząt;
- elektrownie i inne obiekty elektroenergetyczne;
- inne obiekty będące we właściwości organów administracji rządowej, organów jednostek samorządu terytorialnego, formacji, instytucji państwowych oraz przedsiębiorców i innych jednostek organizacyjnych, których zniszczenie lub uszkodzenie może stanowić zagrożenie dla życia i zdrowia ludzi, dziedzictwa narodowego oraz środowiska w znacznych rozmiarach albo spowodować poważne straty materialne, a także zakłócić funkcjonowanie państwa.

Jedna definicja, jeden akt prawny

Jeśli porównamy terminy: „infrastruktura krytyczna", „obiekty podlegające obowiązkowej ochronie" oraz „obiekty szczególnie ważne dla bezpieczeństwa i obronności państwa", bez trudu zauważymy, że kryją się za nimi bez mała tożsame obszary, obiekty niezmiernie ważne dla funkcjonowania państwa i tym samym wymagające szczególnej ochrony (tabela 1), a przy tym spełniające kryteria infrastruktury krytycznej zawarte w dyrektywie Rady UE. W jej rozumieniu infrastruktura krytyczna „oznacza składnik, system lub część infrastruktury zlokalizowane na terytorium państw członkowskich, które mają podstawowe znaczenie dla utrzymania niezbędnych funkcji społecznych, zdrowia, bezpieczeństwa, ochrony, dobrobytu materialnego lub społecznego ludności oraz których zakłócenie lub zniszczenie miałoby istotny wpływ na dane państwo członkowskie w wyniku utracenia tych funkcji"[19].

Tabela 1. Porównanie terminów, za którymi kryją się obiekty niezmiernie ważne dla funkcjonowania państwa

Ustawa „O zarządzaniu kryzysowym"	Ustawa „O ochronie osób i mienia"	Rozporządzenie Rady Ministrów
Art. 3. 2) infrastrukturze krytycznej – należy przez to rozumieć systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców.	Art. 5.1. Obszary, obiekty i urządzenia ważne dla obronności, interesu gospodarczego państwa, bezpieczeństwa publicznego i innych ważnych interesów państwa.	§ 1.1. Rozporządzenie określa obiekty szczególnie ważne dla bezpieczeństwa i obronności państwa, ich kategorie, a także zadania w zakresie ich szczególnej ochrony oraz właściwość organów w tych sprawach.

[19] *Dyrektywa Rady 2008/114/WE z 8 grudnia 2008 r...*, art. 2, pkt a.

Mamy więc trzy akty prawne odnoszące się do tej samej kategorii obiektów, których wykazy (kwalifikowanie) sporządzane są przez te same naczelne organy administracji państwowej (tabela 2).

Tabela 2. Organa kwalifikujące obiekty szczególnej ochrony

Ustawa „O zarządzaniu kryzysowym”	Ustawa „O ochronie osób i mienia”	Rozporządzenie Rady Ministrów
Art. 5b, ust. 7 Dyrektor Rządowego Centrum Bezpieczeństwa: „1) na podstawie szczegółowych kryteriów, o których mowa w ust. 2 pkt 3, we współpracy z odpowiednimi ministrami odpowiedzialnymi za systemy, sporządza jednolity wykaz obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy;	Art. 5 3. Szczegółowe wykazy obszarów, obiektów i urządzeń, o których mowa w ust. 2, sporządzają: Prezes Narodowego Banku Polskiego, Krajowa Rada Radiofonii i Telewizji, ministrowie, kierownicy urzędów centralnych i wojewodowie w stosunku do podległych, podporządkowanych lub nadzorowanych jednostek organizacyjnych.	§ 4.1. Rada Ministrów ustala wykaz obiektów uznanych za szczególnie ważne dla bezpieczeństwa i obronności państwa. 2. Z wnioskiem o uznanie obiektu za szczególnie ważny dla bezpieczeństwa i obronności państwa mogą występować: 1) szef Kancelarii Prezesa Rady Ministrów [...]; 2) ministrowie i przewodniczący komitetów wchodzących w skład Rady Ministrów [...]; 3) prezes Narodowego Banku Polskiego; 4) prezes Zarządu Banku Gospodarstwa Krajowego [...]; 5) wojewodowie [...].

Zasadne wydaje się pytanie: czy nie powinien powstać jeden dokument, w którym zostałoby ujednolicone nie tylko nazewnictwo, ale i organy kwalifikujące obiekty do infrastruktury krytycznej, formacje ochrony, zasady ich tworzenia, działania, ochrony itp. kwestie, bez których bezpieczeństwo tych kluczowych obiektów jest iluzoryczne?

Odpowiedź może być tylko jedna – zdecydowanie tak. Decyzją Rady Europejskiej to państwa członkowskie są odpowiedzialne za koordynację przygotowań do ochrony infrastruktury krytycznej znajdującej się na ich terytorium, a więc także za koordynację aktów prawnych: „Władze państw członkowskich zapewnią przywództwo i koordynację w opracowywaniu i wdrażaniu spójnego podejścia krajowego do ochrony infrastruktury krytycznej w obszarach ich jurysdykcji, z uwzględnieniem istniejących kompetencji wspólnotowych”[20].

Ta powinność spoczywa na Radzie Ministrów RP, tym bardziej że „Do zadań Rady Ministrów wykonywanych w ramach zapewnienia zewnętrznego bezpieczeństwa państwa i sprawowania ogólnego kierownictwa w dziedzinie obronności kraju należy w szczególności: […] 5) określenie obiektów szczególnie ważnych dla bezpieczeństwa państwa, w tym obronności, oraz przygotowanie ich szczególnej ochrony”[21]. Jeśli do infrastruktury włączymy „obiekty szczególnie ważne dla bezpieczeństwa i obronności państwa” oraz „obiekty podlegające obowiązkowej ochronie”, będzie to zadanie dla dyrektora Rządowego Centrum Bezpieczeństwa – pod warunkiem, że dostrzeżone zostaną trzy zasadnicze kwestie.

1. Istnienie trzech aktów prawnych, które dotyczą tej samej sfery: ochrony obiektów szczególnie ważnych dla bezpieczeństwa i sprawnego funkcjonowania państwa. Można przypuszczać, że jest to efekt tzw. inflacji prawa: „– Przyczyny inflacji prawa to nie tylko potrzeby społeczne czy gospodarcze ani konieczność dopasowania krajowych przepisów do unijnych, ale również słabość procesu prawodawczego – diagnozuje dr Grzegorz Wierczyński z Wydziału Prawa i Administracji Uniwersytetu

[20] *Decyzja Rady z 12 lutego 2007 r.*..., pkt 10.
[21] *Ustawa z 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczpospolitej Polskiej, tekst jednolity*, Dz.U. 2004, nr 241, poz. 2416, art. 6.

Gdańskiego. Wskazuje na wielość i rozproszenie instytucji zajmujących się oceną jakości projektowanych regulacji, działających niezależnie od siebie i nietworzących spójnego systemu"[22].

2. Współczesne zagrożenia, możliwość ich wystąpienia bez wcześniejszych oznak, zapowiedzi, a także ich gwałtowny przebieg, co wymusza inne spojrzenie na bezpieczeństwo państwa oraz obywateli: wszystkie przedsięwzięcia w tej dziedzinie muszą być realizowane, „działać" już teraz, w każdej chwili, bez rozgraniczania na czas pokoju czy wojny.
3. Ustawa „O ochronie osób i mienia" oraz ustawa „O zarządzaniu kryzysowym" obowiązują w czasie pokoju: „Zasadnicza różnica pomiędzy szczególną ochroną a obowiązkową polega na tym, że pierwsza prowadzona jest na wypadek zagrożenia bezpieczeństwa państwa i wojny, zaś obowiązkowa ochrona prowadzona jest w czasie pokoju"[23].

Narodowy Program Ochrony Infrastruktury Krytycznej, jak nazwa wskazuje, ma być narodowy, a nie resortowy. Ma być dokumentem, „w którym Rząd przedstawi swoją wizję ochrony kluczowych dla funkcjonowania państwa składników infrastruktury państwa, charakterystykę systemów IK, metodykę oceny ryzyka zakłócenia funkcjonowania IK oraz priorytety, jakimi kierować się powinni uczestnicy OIK. Opisany zostanie ponadto sposób współpracy między sektorem publicznym i prywatnym w OIK na poziomach strategicznym i operacyjnym, a także wskazane zostaną standardy ochrony IK oraz projekty w zakresie badań i rozwoju w tym zakresie"[24].

Pozostaje mieć nadzieję, że – wzorem Departamentu Zarządzania Kryzysowego MSWiA w poprzednich latach – dalsze prace w zakresie ochrony infrastruktury krytycznej będą konsultowane z MON, MSWiA, właścicielami i posiadaczami samoistnymi i zależnymi obiektów, instalacji lub urządzeń infrastruktury krytycznej. Zobowiązuje do tego nie tylko zapis w rozporządzeniu w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej oraz zapowiedzi powołania tzw. forum publiczno-prywatnego, ale i zdrowy rozsądek. Nikt bowiem nie powinien mieć złudzeń, że jesteśmy na początku drogi do budowania spójnego i adekwatnego do rzeczywistych zagrożeń systemu ochrony infrastruktury krytycznej. Małym pocieszeniem jest to, że nie tylko my: „Trwającą od lat dyskusję w politycznych kuluarach Bonn, a później Berlina, na temat obecności militarnej USA w Europie spotęgował niedawny raport Amerykańskiej Federacji Naukowców (FAS). Oceniono w nim, że broń atomowa, przechowywana przez USA w bazach europejskich sojuszników, jest niedostatecznie zabezpieczona, począwszy od zdezelowanych płotów, oświetlenia i «niestabilnych zabudowań», na kiepskim systemie alarmowym i niedostatecznie wyszkolonej załodze skończywszy"[25].

[22] I. Walencik, *Parlament i rząd tworzą coraz więcej złego prawa*, „Rzeczpospolita" 2011, nr 12.
[23] Z. Solejko, *Teoretyczne i praktyczne problemy ochrony infrastruktury krytycznej*, w: *Wyzwania bezpieczeństwa cywilnego XXI wieku – inżynieria działań w obszarach nauki, dydaktyki i praktyki*, Warszawa 2007, s. 281.
[24] M. Pyznar, *Narodowy Program Ochrony Infrastruktury Krytycznej w systemie ochrony tej infrastruktury – wizja Rządowego Centrum Bezpieczeństwa*, w: *Ochrona infrastruktury krytycznej*, red. A. Tyburska, Wyższa Szkoła Policji, Szczytno 2010, s. 111.
[25] P. Cywiński, *Amerykanie do domu!*, „Wprost" 2008, nr 29.

The critical infrastructure – the next council kingdom?

Summary

The article presents origin, history and definition of the high value infrastructure and facilities particularly important for the security and defense of the state, and also of the objects covered by the mandatory security. Key terms and their running in the compliance with the Polish and European Union legislation were explained. Suggestions of the most important changes, which would make the security better are presented. It turns out that there are three acts relating to objects important for state's security. The solution was offered – one document which standardizes nomenclature and departments.